U OVOM POGLAVLJU

- Napad na sisteme e-pošte
- Napad na trenutno razmenjivanje poruka
- Napad na aplikacije protokola za prenos glasa (VOIP)

Poglavlje **14**

Sistemi za komunikaciju i razmenu poruka

Sistemi i protokoli za komunikaciju, poput e-pošte i protokola za prenos glasa preko Interneta, često su nosioci slabih tačaka koje se lako previde. Zašto? Prema sopstvenom iskustvu, komunikacioni softver – kako kod servera, tako i kod klijenta – ranjiv je jer administratori mreže često veruju da su mrežna barijera i softver za zaštitu od zlonamernih programa sve što im je potrebno da se izbegnu problemi ili jednostavno zaborave da zaštite ove sisteme.

U ovom poglavlju, pokazaću vam kako da testirate uobičajene probleme sa e-poštom i VoIP (engl. *voice over internet protocol, VoIP*). Takođe ću istaći i prikaz ključnih mera zaštite koje će vam pomoći da sprečite hakovanje ovih sistema.

Uvod u ranjivosti sistema za razmenu poruka

Gotovo sve aplikacije za prenos poruka predstavljaju metu za hakere na vašoj mreži. Imajući u vidu sve širu upotrebu e-pošte, kao i to koliko poslovanje zavisi od iste, sve vrlo lako može postati meta. Isto važi i za VoIP. Potpuno je zastrašujuće šta ljudi sa zlom namerom mogu da učine sa ovim alatkama.

Kod sistema za razmenu poruka, jedna od osnovnih slabosti je ta što većina protokola za podršku nije osmišljena uzimajući zaštitu u obzir – posebno oni koji su se pojavili pre nekoliko decenija kada sigurnost nije bila ni blizu značajna kao u današnje vreme. Zanimljivo je da su čak i moderni sistemi za razmenu poruka – ili barem primena protokola – *još uvek* podložni ozbiljnim sigurnosnim rizicima. Sem toga, pogodnost i upotrebljivost često prevagnu nad potrebom za sigurnošću.

Mnogi napadi na sisteme za razmenu poruka su samo blage neprijatnosti; ostali mogu da nanesu ozbiljnu štetu podacima i ugledu vaše organizacije. Zlonamerni napadi na sisteme za razmenu poruka su sledeći:

- Prosleđivanje zlonamernih programa (softvera).
- Rušenje servera.
- Zadobijanje daljinske kontrole nad radnim stanicama.
- Hvatanje informacija koje putuju mrežom.
- Pažljivo proučavanje e-pošte sačuvane na serveru i u radnim stanicama.
- Prikupljanje informacija o razmeni poruka preko dnevničkih datoteka ili analizatora mreže, a to napadaču može da pruži informacije o razgovorima između ljudi i organizacija (što se često naziva analizom saobraćaja ili analizom društvenih mreža).
- Preuzimanje i preslušavanje telefonskih razgovora.
- Prikupljanje informacija o unutrašnjoj konfiguraciji mreže, kao što su ime računara i *IP* adrese.

Ovakvi napadi mogu dovesti do problema kao što je neovlašćeno – a moguće i protivzakonito – otkrivanje poverljivih informacija, kao i gubitak istih.

Prepoznavanje i borba protiv napada na e-poštu

Napadi koje predstavljam u ovom odeljku koriste najčešće ranjivosti e-pošte za koje znam. Dobra vest je da većinu možete ukloniti ili ublažiti do te mere da ne predstavljaju rizik za informacije. Neki od ovih napada zahtevaju poznavanje osnovnih metodologija hakovanja: prikupljanje javnih informacija, skeniranje i popisivanje sistema, pronalaženje i korišćenje ranjivosti. Ostali napadi se mogu izvesti slanjem e-pošte ili preuzimanjem mrežnog saobraćaja.

Bombardovanje e-poštom

Bombardovanje elektronskim pismima (engl. *email bombs*) napada tako što stvara uslove za uskraćivanje usluge (engl. *denial of service*, DoS) na vašem softveru za e-poštu, čak i na mreži i Internet konekciji jer zauzimaju veliki deo propusnog opsega, a ponekad i skladišnog prostora. Bombe u vidu e-pošte mogu da dovedu

do pada servera i omoguće neovlašćeni administratorski pristup – da, čak i uz današnje naizgled beskrajne kapacitete memorije.

Priložena datoteka

Napadač može izvesti napad pretrpavanjem priloženim datotekama tako što će poslati na stotine ili hiljade pisama sa izuzetno velikim prilozima za jednog ili više primaoca na vašoj mreži.

NAPADI PRILOŽENIM DATOTEKAMA E-POŠTE

Napadi priloženim datotekama imaju dva cilja:

- **Server za poštu može biti meta sa ciljem** potpunog prekida rada na sledeće načine:
  - *Prepunjenost memorije:* Više velikih poruka mogu brzo da popune kapacitet servera pošte. Ako se poruke ne obrišu automatski putem servera ili ručno od strane pojedinačnih korisničkih naloga, server neće biti u mogućnosti da primi nove poruke.

    Ovakav napad može da dovede do ozbiljnog *DoS* problema po vaš sistem pošte, pri čemu će doći ili do pada sistema ili ćete dobiti zahtev za prekidanje veze sa internetom da biste očistili nagomilanu poštu (engl. *junk*). 100MB priložene datoteke koja se pošalje deset puta za stotinu korisnika može da zauzme 100GB skladišnog prostora, a može i više!

    UPOZORENJE
  - *Blokiranje propusnog opsega:* Napadač može da vam nagomilanom poštom potpuno zaustavi ili uspori prijem pošte. Čak i ako vaš sistem automatski prepoznaje i odbacuje očigledne napade prilozima, lažne poruke troše resurse i usporavaju prenos validnih poruka.
- **Napad na pojedinačnu adresu e-pošte** može imati ozbiljne posledice ako adresa pripada bitnom korisniku ili grupi.

MERE PROTIV NAPADA PRILOŽENIM DATOTEKAMA

Sledeće mere zaštite mogu pomoći u sprečavanju napada pretrpavanjem priloženim datotekama:

- **Ograničavanje veličine pošte ili priloženih datoteka.** Potražite ovu opciju u podešavanjima konfiguracije servera pošte (ima ih u *Microsoft Exchange-u*), u delu za filtriranje poruka ili u podešavanju klijenta.
- **Ograničavanje prostora svakog korisnika na serveru ili u oblaku** (engl. *cloud*)**.** Ova mera zaštite sprečava upisivanje velikih priloženih datoteka na disk. Ograničite veličinu poruka za dolazne, pa čak i odlazne poruke ako imate za cilj da sprečite korisnika da izvrši ovaj napad unutar vaše mreže. Smatram da je nekoliko gigabajta dobro ograničenje, ali ono zavisi od veličine vaše mreže, raspoloživosti skladištenja, kulture poslovanja i tako dalje. Razmislite pažljivo o ograničenju pre nego što ga zadate.

SAVET

Razmotrite korišćenje *SFTP*, *FTPS* ili *HTTPS* umesto pošte za prenos velikih datoteka. Dostupne su mnoge usluge za prenos datoteka u oblaku, kao na primer *Dropbox for Business*, *OneDrive for Business* i *Sharefile*. Takođe možete podstaći korisnike da koriste zajedničke ili javne foldere. Na taj način možete sačuvati kopiju datoteke na serveru, a primalac može da preuzme datoteku na svojoj radnoj stanici.

UPOZORENJE

Suprotno uvreženom verovanju i upotrebi, sistem pošte *ne treba* da bude spremište informacija, ali se pošta upravo u to razvila. Server pošte koji se koristi za ovu svrhu može dovesti do bespotrebnih nezakonitih i regulatornih rizika i pretvoriti se u veliku noćnu moru ako vaša organizacija primi zahtev za uvid u vaš sistem pošte od nadležnih organa. Važan deo vašeg sistema bezbednosti je raspodela i upravljanje podacima. Ali ne bavite se time sami. Aganžujte advokata, menadžera za ljudske resurse i šefa informativne službe. To vam omogućava da pravi ljudi budu prisutni i da vaš posao ne upadne u nevolju zbog posedovanja previše – ili premalo – elektronskih podataka u slučaju da dođe do tužbe ili istražnog postupka.

Veze

Haker može istovremeno poslati ogroman broj pisama na vaš sistem pošte. Zlonamerni program prisutan na vašoj mreži može isto to da uradi iz unutrašnjosti mreže ako mreža ima otvoren jednostavan protokol za prenos pošte (*Simple Mail Transfer Protocol*, *SMTP* protokol), što često i jeste slučaj. Ovi napadi na veze mogu dovesti do toga da server odustane od obrade svih dolaznih ili odlaznih zahteva za protokol za kontrolu prenosa (*Transmission Control Protocol*, *TCP* protokol). U ovom slučaju može doći do zaključavanja ili pada servera, a to omogućava napadaču da dobije administratorski ili korenski (engl. *root*) pristup sistemu ili da pristupi kao administrator.

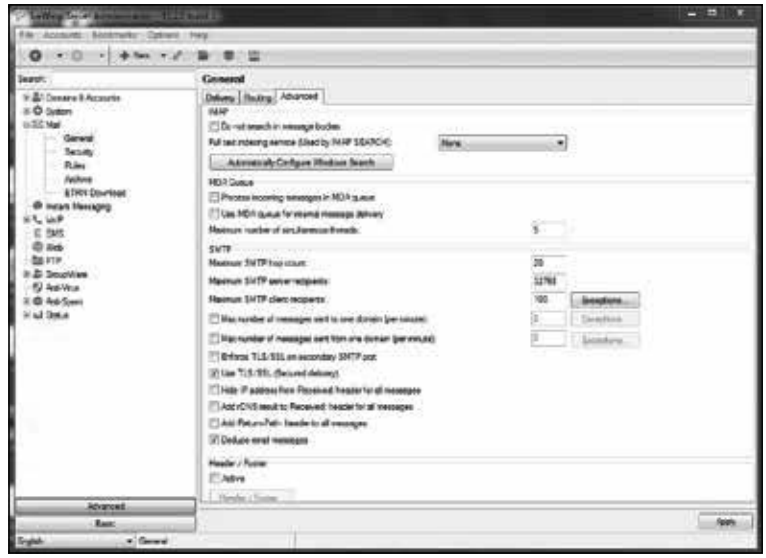
NAPADI PUTEM PREPLAVLJIVANJA E-POŠTOM

Napad pri kojem se koristi preplavljivanje e-poštom često se izvodi kao napad neželjenom poštom (engl. *spam*) i ostalim vrstama *DoS* napada.

MERE PROTIV NAPADA NA VEZE

Treba sprečiti napade na poštu što je moguće više po obodu mreže, najbolje u oblaku. Što više mrežnog saobraćaja ili zlonamernog ponašanja držite podalje od servera pošte i klijenata, utoliko bolje.

Mnogi serveri e-pošte imaju opciju ograničavanja broja resursa koji se koriste za dolazne veze, kao što je prikazano na Slici 14-1 kod podešavanja maksimalnog broja istovremenih programskih niti za *IceWarp* server pošte. Ovo podešavanje ima različite nazive za različite servere pošte i mrežne barijere, te je dobro proveriti šta piše u dokumentaciji. Potpuno zaustavljanje neograničenog broja dolaznih zahteva može biti nemoguć zadatak, ali možete ublažiti uticaj napada. Ovo podešavanje ograničava vreme serverskog procesa što pomaže za vreme *DoS* napada.



SLIKA 14-1: Ograničavanje broja resursa koji obrađuju dolazne poruke.

Čak i u velikim kompanijama ili prilikom korišćenja servisa za poštu u oblaku, kao što su *G Suite* ili *Office 365*, gotovo da nema razloga da na hiljade dolaznih pisama bude neophodno u kratkom vremenskom periodu.

UPOZORENJE

Serveri e-pošte mogu da se programiraju da dostavljaju pisma serveru za automatizovane funkcije, na primer *napravite ovu porudžbinu vezanu za e-trgovinu kada primite poruku sa ovog naloga*. Ako DoS zaštita nije deo sistema, napadač može srušiti i server i aplikaciju koja prima te poruke i tada postoji mogućnost da dođe do zakonskih prekršaja kod e-trgovine. Ovaj tip napada lakše se sprovodi na veb lokacijama e-trgovine koje u obrascima ne koriste znakovni test *CAPTCHA* (*Completely Automated Public Turing test to tell Computers and Humans Apart*), test koji otkriva da li je posetilac čovek ili program. To može biti problem kada vršite skeniranje ranjivosti na vebu preko veb obrazaca koji su vezani za adrese e-pošte u pozadini. U takvoj situaciji nije neuobičajeno da se dobije na hiljade, ako ne i milion, pisama. Isplati se biti pripremljen i obavestiti sve koji su uključeni u to da rizik postoji. U Poglavlju 15 ću objasniti zaštitu veb aplikacija..

Automatizovanje kontrole sigurnosti e-pošte

Možete primeniti sledeće mere kao dodatnu zaštitu sistema e-pošte:

- **Zadrška:** Zadrška (engl. *tarpitting*) prepoznaje dolazne poruke namenjene nepoznatim korisnicima. Ako vaš server pošte podržava zadršku, može vam pomoći u sprečavanju napada na server u vidu neželjene pošte ili kod *DoS* napada. Ako se prekorači unapred definisan prag – recimo, više od 100 poruka u minuti – funkcija zadrške uspešno zaustavlja saobraćaj sa *IP* adrese pošiljaoca na određeni period.

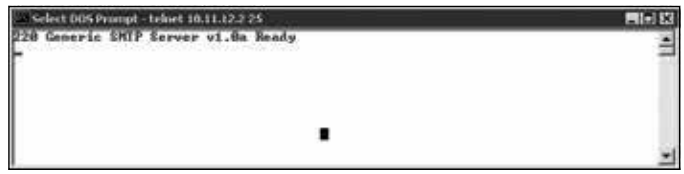
- **Mrežna barijera e-pošte:** Mrežne barijere pošte i aplikacije za filtriranje na osnovu sadržaja kupljene od firmi kao što su *Symantec* i *Barracuda Networks* dosta pomažu u sprečavanju različitih napada na poštu. Ove alatke štite gotovo sve aspekte sistema pošte.
- **Zaštita na obodu:** Iako nisu karakteristični za e-poštu, mnoge mrežne barijere i sistemi za sprečavanje upada mogu da prepoznaju različite napade na poštu i zaustave napadača u realnom vremenu, što dobro dođe za vreme napada.
- **CAPTCHA:** Korišćenje *CAPTCHE* kod veb obrazaca e-pošte pomaže pri umanjivanju uticaja automatizovanih napada i smanjuje šanse za prenatrpavanje poštom i DoS, čak i kada obavljate naizgled bezazleno skeniranje ranjivosti mreže. Ove prednosti dobro dođu prilikom testiranja veb lokacija i aplikacija, o čemu govorim u Poglavlju 15.

Zaglavlja

Prilikom hakovanja servera e-pošte, prioritet hakera je da otvori zaglavlje (engl. *banner*) da bi video da li može da otkrije koji softver koristi server pošte. Ovakva provera je jedna od najkritičnijih da bi se saznalo koje informacije javnost ima o vašim *SMTP*, *POP3* i *IMAP* serverima.

Prikupljanje informacija

Na slici 14-2 prikazano je zaglavlje na serveru pošte kada se ostvari osnovna *Telnet* veza na priključku 25 (*SMTP*). Da biste ovo dobili na komandnoj liniji unesite **telnet** ip ***ili_ime_vašeg_servea* 25**. Ova komanda otvara *Telnet* sesiju na *TCP* priključku 25.



SLIKA 14-2: *SMTP* zaglavlje koje prikazuje informacije o verziji servera.

Vrsta softvera e-pošte i verzija servera su često prilično očigledni i hakerima pružaju ideje o mogućim napadima, pogotovo ako pretražuju bazu podataka da bi pronašli ranjivosti koje su već poznate u toj verziji softvera. Slika 14-3 prikazuje isti server pošte sa *SMTP* zaglavljem koje je promenjeno iz unapred zadatog (u redu, i prethodno je takođe) da bi se prikrile informacije verzije servera pošte.

SAVET

Možete prikupiti informacije o *POP3* i *IMAP* uslugama pošte koristeći *Telnet* za priključak 143 110 (*POP3*) ili priključak 143 (*IMAP*).